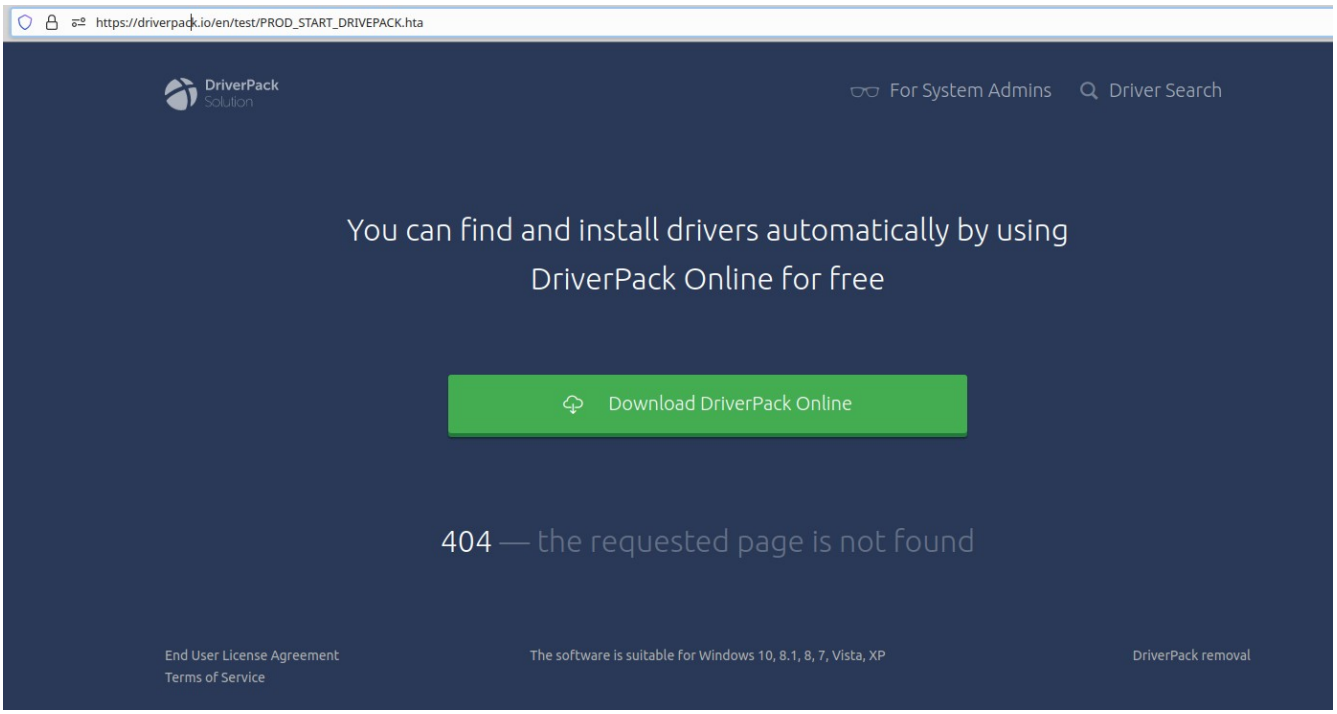
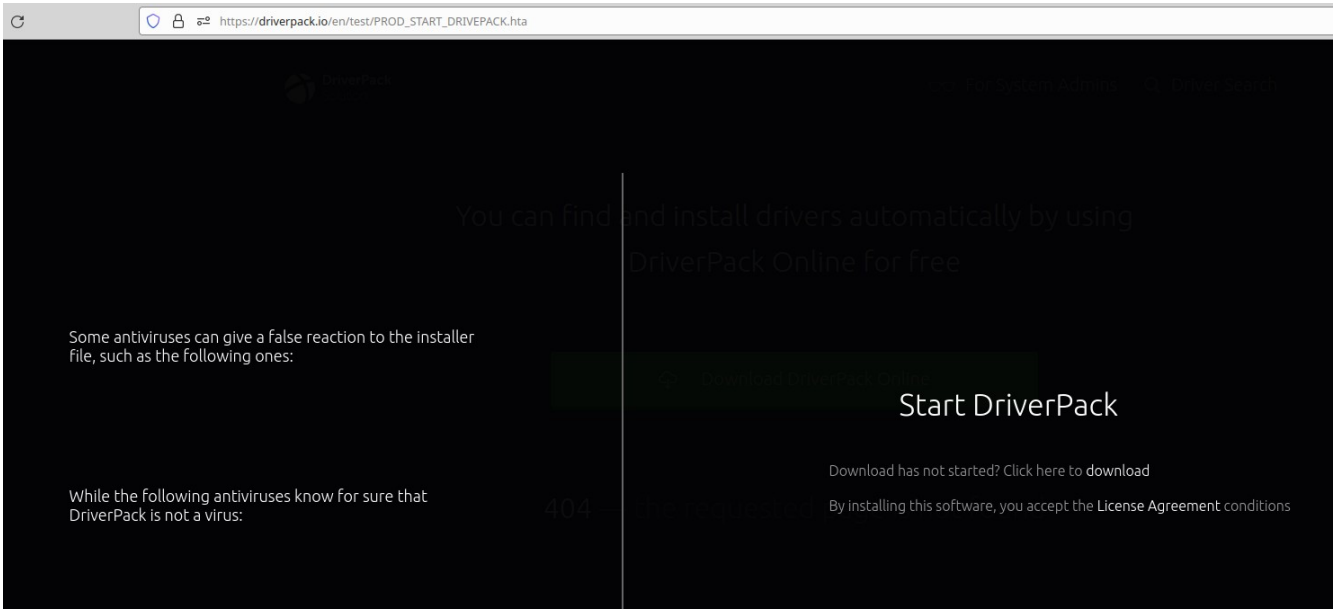
MSHTA.exe Suspicious Activity Investigation

User [redacted] went to the website of "dl.driverpack[.]io/test/PROD_SERVER_DRIVERPACK.hta" which downloaded and ran the HTA file. This website seems to be down. However we found that if you remove the subdomain (which seemed to be a redirect it takes you to "https://driverpack[.]io/en/test/PROD_START_DRIVEPACK.hta" and connects to the same websites seen in the logs.

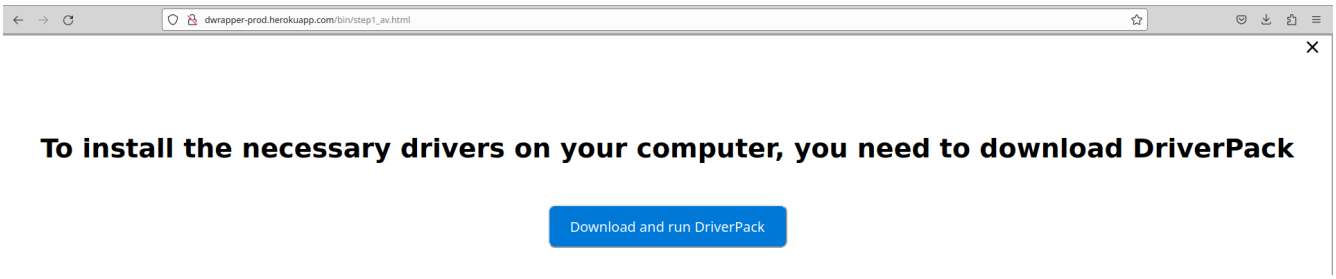


after clicking the "Download DriverPack Online" button it downloads the file and shows this on the screen.



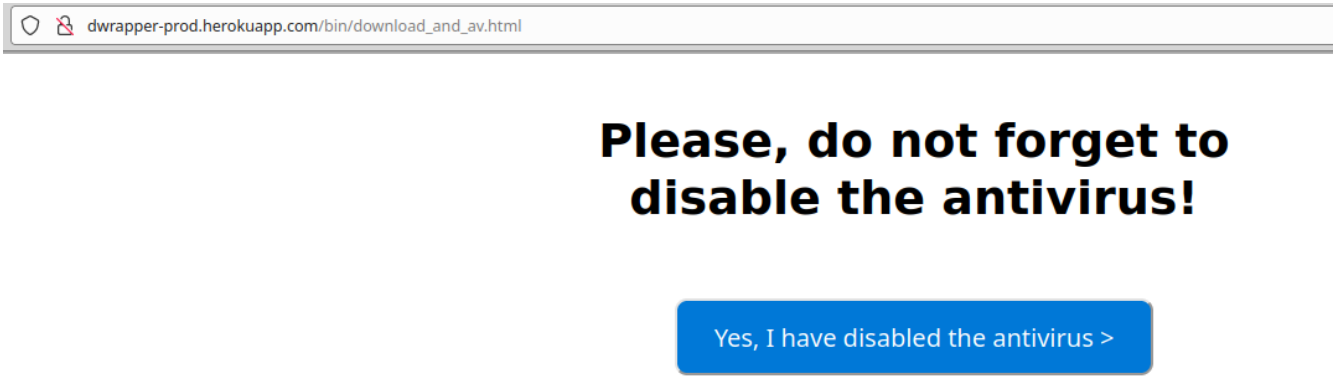
If you run the HTA file it will automatically use MSHTA.exe and open
“http://dwrapper-prod.herokuapp[.]com/bin/step1_av.html”

When I browsed to:
“http://dwrapper-prod.herokuapp[.]com/bin/step1_av.html”
I was presented with a prompt. Following the prompt only allowed me to get to the next window.



Screenshot from step1_av.html

step1_av.html redirects to:
“http://dwrapper-prod.herokuapp[.]com/bin/download_and_av.html”



Screenshot from download_and_av.html

When I examined the webpage I can see that it starts the following Java Scripts:

1. http://dwrapper-prod.herokuapp[.]com/client_ip.js
2. http://dwrapper-prod.herokuapp[.]com/bin/src/missing-scripts-detector.js
3. http://dwrapper-prod.herokuapp[.]com/bin/src/variables.js
4. http://dwrapper-prod.herokuapp[.]com/bin/src/variables/1.js
5. http://dwrapper-prod.herokuapp[.]com/bin/src/variables/2.js
6. http://dwrapper-prod.herokuapp[.]com/bin/src/variables/3.js
7. http://dwrapper-prod.herokuapp[.]com/bin/src/variables/4.js
8. http://dwrapper-prod.herokuapp[.]com/bin/src/variables/5.js
9. http://dwrapper-prod.herokuapp[.]com/bin/src/script.js
10. http://dwrapper-prod.herokuapp[.]com/bin/src/statistics.js
11. http://dwrapper-prod.herokuapp[.]com/bin/src/lang.js
12. http://dwrapper-prod.herokuapp[.]com/bin/src/download.js
13. http://dwrapper-prod.herokuapp[.]com/bin/src/systeminfo.js

14. http://dwrapper-prod.herokuapp[.]com/bin/src/av.js

Note: Several of these scripts have Russian Language in them.

Summary Overview of the Java Scripts:
client_ip.js: returns the public IP address of the device visiting it.
missing-scripts-detector.js: verifies scripts have run. Also has a function called "showScreenDisabledAntivirus"
variables.js**:** seems to be a combination of 1.js through 4.js as a single script.
1.js: looks for the following registry key:

- HKCU\SOFTWARE\dwrapper

2.js: enumerating the device.

- Checks the directory that HTA file is in
- Checks architecture looking for 64 bit
- Checks service packs installed
- Checks internet explorer version
- Checks java script version.

3.js: Has a "category" called "Wrapper / Antivirus blocks". Is looking for the following registry keys:

- HKLM\SOFTWARE\Microsoft\
- HKLM\SOFTWARE\Microsoft\
- HKLM\SOFTWARE\Wow6432Node\Microsoft\
- HKCU\SOFTWARE\Microsoft\
- HKCU\SOFTWARE\Microsoft\
- HKCU\SOFTWARE\Wow6432Node\Microsoft\

4.js: reads and edits registry

- "HKLM\SOFTWARE\Clients\StartMenuInternet\"
- "HKLM\SOFTWARE\Clients\StartMenuInternet\<Browser Name>\shell\open\command"

5.js: checks to make sure a document is ready and reads it. Possible data exfiltration.
script.js: Checks screen size and if it can be changed (possibly looking for Honey Pot), checks if it has admin rights, looks for and runs HTA file.
statistics.js: lots of Russian. Enumerates device information and seems to connect to a website tracking api:

- http://example-dwrapper.matomo[.]cloud/matomo.php

lang.js: determines the language you are using so that it can present the information in the correct language. Also reads the following registry key:

- HKCU\Control Panel\International\Locale

download.js: attempts to download two files, if it is bot able to because Antivirus is blocking it, then it will present a webpage in Russian to download the software from. The code shows these files would be later deleted. The following are the two files it is looking to save on the computer.:

- log_bits_start.txt
- log_bits_info.txt

systeminfo.js: enumerates a lot of information about the host system including up time, installation date, local time and date, OS version, AV version, country code, languages installed, service packs installed, , software installed, what it is used for (domain controller, server, workstation), etc. looks at the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Signature Updates\ EngineVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Signature Updates\ AVSignatureVersion

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Signature Updates\ ASSignatureVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProductName
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ DisplayVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ CurrentBuild
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ CurrentBuild
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ EditionID
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ CompositionEditionID
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ BuildNumber

av.js: checks version of antivirus and if it is disabled.